PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
G06F

A2

(11) International Publication Number: WO 00/62140

(43) International Publication Date: 19 October 2000 (19.10.00)

(21) International Application Number: PCT/CA00/00406

(22) International Filing Date: 12 April 2000 (12.04.00)

(30) Priority Data:
60/128,871 12 April 1999 (12.04.99) US

(71) Applicant: SILANIS TECHNOLOGY INC. [CA/CA]; 3333 Côte Vertu, Suite 450, St-Laurent, Quebec H4R 2N1 (CA).

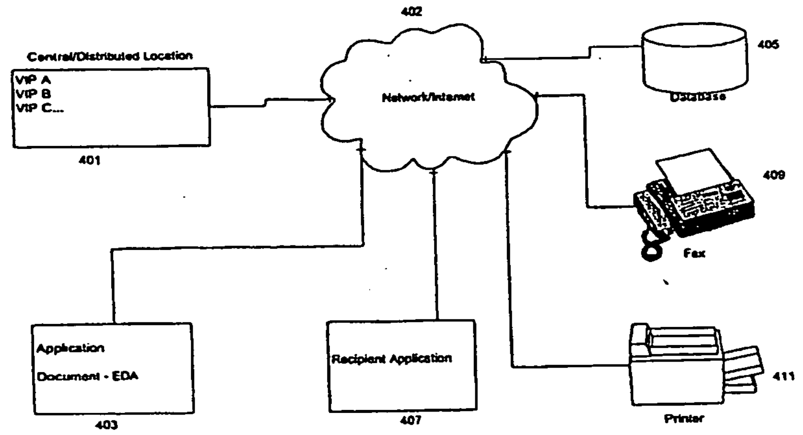
(72) Inventors: SILVESTER, Joseph; 282 Place des Cèdres, Dollard des Ormeaux, Quebec H9G 1W1 (CA). PETROGIANNIS, Tommy; 4560 Cumberland Avenue, Montreal, Quebec H4B 2L4 (CA). LEBLANC, François; 3770 Ave. Laval, Montreal, Quebec H2W 2H7 (CA). DUMAIS, Guy; 9181 Millen, Montreal, Quebec H2M 1W8 (CA). GOUDREAULT-EDMOND, Benoit; 7349 Ave. Azilda, Anjou, Quebec H1K 3A4 (CA). LAURIE, Michael; 4827 Meloche, Pierrefonds, Quebec H9J 1Y9 (CA). MILCZAREK, Ed; 5135 des Cageux, Pierrefonds, Quebec H9J 3C4 (CA).

(74) Agent: ROBIC; 55 Saint-Jacques, Montreal, Quebec H2Y 3X2 (CA).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: SECURE ELECTRONIC DOCUMENT CREATION, APPROVAL AND DISTRIBUTION METHOD IN AN OPEN AND DISTRIBUTED NETWORK ENVIRONMENT



(57) Abstract

The invention concerns a system and method for the secure creation, approval and distribution of electronic documents in an open and distributed network environment. Personal information of a user for whom a profile is being created; identity verification data; and relevant data regarding the user are obtained in order to create a virtual identification profile (VIP). The information is updated and edited and a variable authentication code (VAC) related to this information is calculated. The VIP is then encrypted, and a central location is updated with the information. The VIP can be used in a system which includes a central location for storing and updating a plurality of VIPs, and at least one application for creating a document, the application being in communication with the central location. The application verifies if the VIP contains pertinent data for the user and for inserting the pertinent data into the document at the time of creation and for approving the document once created. Consequently, if the document is transmitted to someone else or to another application, an embedded application can verify the VAC in order to determine if the document has been modified since its approval. It is thus possible to bind a signature or logo forming part of the VIP in order to distribute electronic documents in an open system, while preserving security.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

SECURE ELECTRONIC DOCUMENT CREATION, APPROVAL AND DISTRIBUTION METHOD IN AN OPEN AND DISTRIBUTED NETWORK ENVIRONMENT

Field of the invention

The present invention relates to a method for the secure creation, approval and distribution of electronic documents in an open and distributed network environment.

Background of the Invention

Figure 1 show the typical hybrid document environment prevalent in most organizations and corporations. Basically documents originate in one of two ways: they start their existence as a paper document or as an electronic document. In the majority of cases, documents are approved using handwritten signatures and/or seals. These approvals are usually executed on paper documents. Once the paper document has been approved, it is usually stored in a file cabinet or scanned into an electronic file for storage. The paper documents are distributed via fax, courier or mail service. In general, original documents are the documents that are signed or sealed, and tend to be stored by the organization for legal reasons. Therefore, documents that are approved on paper or originated on paper are extremely hard to eliminate once they have been created and approved.

Most corporations and organizations in North America and Europe have now adopted computers and networks. The advent of Internet is further accelerating the adoption of computers into homes and businesses. However, the majority of the information is still created, approved, stored and distributed on paper documents. Paper is extremely expensive and difficult to store, handle and distribute. However, paper does have universal acceptance throughout the world and there are established infrastructures and procedures in place to facilitate the storing, distribution and handling of paper documents.

Organizations and corporations have customized letterheads to show the proper source of document. Only people who work for these organizations will typically have access to these special letterheads. Additionally, if the contents of the document are important, the document will have to be signed or approved by someone. Also, in order for the document to be valid it may need to be signed by someone at a certain level. In other cases, there have to be multiple signatures for the document to be valid. The document might also require multiple signatures and notarization for independent verification of the document. For some documents to be valid, a company seal has to be applied to the document. The idea behind the seal is that even if someone has access to the letterheads of the company, the seal is usually only available to a trusted authority and to reproduce the seal is more difficult than it is to reproduce the letterhead. This is another security measure to try and prevent the possibility of fraud in the organization. Certain document such as bank notes, are unique and serialized, and may also have designs, which makes them difficult to copy or reproduce.

There is however, to Applicant's knowledge, no product that provides the equivalent electronic solution to letterhead and signatures. Specifically, particularly when it comes to email, serious limitations exist with respect to its use. Basically, an organisation or person can represent itself in email in one of two basic ways: by a text string or via an embedded or linked graphic that represents a corporate logo.

The problem with both of these approaches is that either they are very impersonal (the text string is generic and can be made to look like any other text string), or the graphic logos have no security attached to them, so that anyone can apply a logo to an email and pass it off as that of the owner of the logo.

A number of solutions have been proposed to approve electronic documents, but they are applicable in a closed system.

However, there has not, to Applicant's knowledge, been developed a solution for securely creating, distributing and approving documents in an open and distributed network environment.

Summary of the Invention:

It is an object of the invention to provide a method for the secure creation, approval and distribution of electronic documents in an open and distributed network environment. In accordance with the invention, this object is achieved with a method for creating a virtual identification profile (VIP), comprising the steps of:

(a) obtaining personal information of a user for whom the profile is being created;

(b) obtaining identity verification data;

(c) obtaining relevant data;

(d) updating and editing the information gathered at steps (a) to (c) and calculating a variable authentication code related to this information;

(e) encrypting the VIP; and

(f) updating a central location with the information contained in the VIP.

The invention also concerns a method for creating a secure document comprising the steps of:

(a) obtaining a virtual identification profile for the user creating the secure document;

(b) determining if the virtual identification profile includes pertinent information;

(c) if so, inserting pertinent information from the virtual identification profile into the document and making the document ready for use;

(d) if not, creating a low level document and making the document ready for use.

Additionally, the invention provides for a method for securely printing a secure document including security information, comprising the steps of:

(a) providing the document within an application;

(b) accessing security information present in the document or associated therewith;

(c) determining if secure print is enabled;
  (i) if not, verifying and inserting security information and printing the document; or
  (ii) if so, determining if a central database is available;
    (1) if not, aborting the print and informing the user;
    (2) if so, verifying if the print counter is less than a predetermined counter;
      if not, aborting the print and informing the user; and
      if so, incrementing the print counter, verifying and inserting security information and printing the document.

A system for creating, approving and distributing secure documents is also contemplated within the present invention, comprising:

a central location for storing and updating a plurality of virtual identification profiles (VIP), each of said virtual identification profiles being linked to a single user, said virtual identification profile including personal information, identity verification data and relevant data, and a variable authentication code associated with a respective VIP; and

at least one application for creating a document, said at least one application being in communication with said central location, said application verifying if said VIP contains pertinent data for the user and for inserting the pertinent data into the document at the time of creation and for approving the document once created.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention and its advantages will be more easily understood after reading the following non-restrictive description of preferred embodiments thereof, made with reference to the following drawings in which:

Figure 1 [prior art] is a schematic representation of the typical current hybrid document environment;

Figure 2 is a flowchart of the steps for creating a VIP according to the invention;

Figure 3 is a flowchart of the steps for creating and verifying a document according to the invention;

Figure 4 is a schematic representation of an EDA according to the invention;

Figure 5 is a schematic representation of secure printing of a document according to the invention; and

Figure 6 is a schematic representation of the system according to a preferred embodiment of the invention.

DESCRIPTION OF A PREFERRED EMBODIMENT OF THE INVENTION

The main focus of the invention is to permit an organization to function in an open environment, i.e. a hybrid document environment as shown in Fig. 1. The key to making this a reality is to use the document/data and/or the delivery system to deliver the secure or secret/controlled information. Another important aspect of this invention is to allow users to work in the same environment as described in Figure 1 with minimal modifications to existing procedures and systems. Consequently, one important aspect of the invention is the provision of a mechanism to validate the contents of the document or the user identification data, using a Variable Authentication Code (VAC). This VAC will be mathematically related to the number of transactions that are done using the data and the different number of users. A further important aspect of the invention is to embed in a document an embedded document application or to provide a link to the document application, as will be further described.

In the context of the present invention, each of the following major components will be examined in detail:

- User/Organization Identification for Approval and Verification purposes
- Secure/Controlled electronic and paper document creation and approval
- Secure/Controlled document printing, storage and distribution

- Secure/Controlled document process and behavior

It should be noted at the outset that the above components can coexist or exist individually in any given system.

User Identification and Organization Identification

The first step of the present invention is to structure a virtual identification profile, hereinafter referred to as "VIP". The VIP contains personal and/or corporate information, verification data, relevant data and a DAC, which is a mathematical representation of the VIP.

Identification of the user can be done using various methods. Typically, depending on the security requirements, all or some of the following items can be used. However, basic information must be present in the VIP: personal information (name, address, etc.); verification data (such as a digitized signature or biometric data); relevant data (ID No.; private/public key pair; digital certificates). It should be apparent that the more items are used, the easier it will be to identify the individual at a later time:

- Name
- Address
- Telephone
- Email
- Title
- Private/Public Key pair
- Passwords
- Single or Multiple Certificates
- Social Security Number
- Medical Insurance Number
- Passport Number
- Other identifying information such as seals, stamps, indicia, etc.
- Photograph

- Digitized Signature
- Biometric Data
    - Voice
    - Signature Dynamics
    - Retinal Image
    - Finger prints
    - Hand metrics
    - Face Metrics
    - DNA sequence
    - Other biometric markers or combination thereof
- Variable Authentication Code (VAC)
- Central Database updated, last updated date, date of last use, etc.
- Additional Data fields – this can define ID of the employer, position (or title) in the company, certificates, private keys, public keys – these fields can be expanded as required. There could also be personal information such as medical records, travel history, inherited VIP files, financial history etc.

The process begins 11 by determining whether or not a new VIP is being created 13. If so, the personal information of the user is obtained and inserted 15, verification data inserted 17, relevant data inserted 19, and data is updated or edited and the VAC is calculated 21. All the information in the VIP is encrypted and stored in a secure environment. It should be noted that the VIP can be a file, record in a database, etc.

If the update is successful 27, the central location is appropriately marked 31. If the update is not successful 35, the creation or update is aborted.

On the other hand, if what is being performed is an update of an existing file, the file is opened 37, and steps 21, 23, 25, and 27 are performed according to the previous description.

The information present in the VIP cannot be added or deleted without user notification 23 and preferably a central location 25. However, certain information such as the VAC will be automatically changed with or without user knowledge or consent depending on the circumstances. Editing and manipulating the information contained in the VIP file will be strictly controlled and recorded by the central location. Optionally, all information can be stored together or separately, as the case may be. For example, medical records and access information could be stored in separate medical locations with appropriate links inside the VIP, as could be financial information, etc.

The data in the VIP is preferably stored in an onion model, i.e. in multiple layers. The outermost layer contains public or low security information. The next layer contains more secure information and the deeper one progresses into the model the more sensitive the data. Each layer can be protected with different encryption schemes, so that decrypting one layer does not mean the entire VIP becomes compromised.

In the present invention, the VIPs have the ability to inherit data from other VIPs. For example, if a Person A with VIP A is employed by company B having the company VIP B, then, by mutual agreement, certain elements or data contained in the VIPs could be exchanged. In other words, the VIP A could inherit public data or data that is to be made available to the employees from the company's VIP B. This can be accomplished using existing methods such as tagging data that can be transferred etc. This exchange of data can be automatic or manual. In the example above the VIP A could inherit the company address, telephone number, encryption code to be used for secure communications etc. Similarly the Company VIP B could inherit pertinent data from the VIP A. This interactive inheritance could occur in various situations such as the one mentioned above.

The VAC will be modified depending the transactions that are performed using this identification file. Anytime independent transactions are performed where this identification file can be identified or linked to the real person, the VAC will be increased. The VAC can be normalized to percentage and each transaction will create a change in the VAC. For example, transactions that are done with government organizations can increase the VAC of the person doing the transaction. As more certificates from other agencies are included, the VAC could be increased. Similarly, the same method could be employed if the person is approving secure documents containing high security contents. The assumption here is that these documents will be highly scrutinized by others: if illegal VIP files are used to approve, this would be reported and corrected. Also, the VAC could be decreased if the VIP file has not been used for certain time.

The VAC can be checked and verified before a transaction is completed. The type of transaction the user will want to participate in will dictate the VAC required. The user may need to provide more personal information to increase the VAC percentage to participate in these transactions or add more data to the VIP to increase the VAC.

The VIP can be created at authorized central locations in an organization or government or private agencies that have the appropriate hardware and software (See Figure 2). The software will determine, depending on the detail in the VIP, what VAC will be assigned to the VIP. In all circumstances, the VAC is intimately related to the contents of the VIP.

The VIP does not have to be a physical file: it could be a record in a database, field, a database entry, web page, web site, a location in memory containing the information, etc. It could be stored in any format as long the information is available for use through a network. The word "file" is used in the context of the present application as a generic term to indicate that the pertinent data is available and accessible for use and is structured.

Secure Document Creation and Approval

In a typical closed environment, document creation and approval can be done using established database access methods. For example, all users and their signatures or identification can be stored in a central database. During the creation of the user signature file, a unique record can be stored in the central database that is linked to the signature file. When a user attempts to sign a document in the closed environment, the approval software will check the unique marker in the signature file with the central database. If the central database does not contain the unique marker, then the user can be prevented from signing the document. A message can be sent to the appropriate authority indicating the fact that an unregistered or uncontrolled signature was being used in the closed environment system. However, for this method to work, the environment has to be closed and the central database needs to be accessible to all the users. Optionally, other identification information can be stored in a central database, such as biometric information, and compared against the person approving to verify the identity of the person. This method and procedure is appropriate only for closed systems, i.e. systems where users will have access to a central database, such as a manufacturing plant, where everyone is connected to a central database. Users can be asked to identify themselves, their identity can be validated using the central database and then appropriate access can be granted.

In a distributed open environment, the closed environment model cannot apply. It has been found that some control and security found in closed systems can be present in an open environment by embedding the required security features and data in the document itself, according to a feature of the present invention (See Figure 3). For example, as a controlled document is created, the document could be signed in a manner similar to code signing and appropriate control information such as public keys of the signers of the document could be inserted therein (assuming people will be approving the document). This would identify the document as originating from a controlled environment, the public key of the company being distributed publicly, anyone wanting to verify the authenticity of the document being able obtain the public key and verify the origin of the document. Additional information could be added to the document in an encrypted fashion, such as the identity or the public keys of the signers or the biometric information of the signers could be inserted into the document. Now, if this document is to be signed outside the closed environment, the approval software can verify the user identity with the ones contained in the document; if they are the same it will permit the approval; if not, it will not allow the users to sign. The above mentioned VIP file could contain the public key of the employer, in addition to private/public key identifying the user.

The same method can be used to protect the contents of the document. The document can be protected using encryption technology. The unlock passwords can be embedded in the document, again related to the users who have access to the document. The application to unlock the document can be a part of the signing application. The unlock procedure would be similar to the signing application, where the user would identify himself/herself using their VIP file and this would be used to unlock and decrypt the encrypted portions of the document.

More specifically, the present invention provides for a method for creating a secure document. Under a given application (such as a word processor, spreadsheet, graphics, etc.), a command is given to initiate the creation of such a secure document 101. A determination is made as to whether the environment is closed or open 103. If the environment is open, a determination is made as to whether the VIP of the user creating the document contains pertinent date to the type of document that is being created 105. If so, such data is inserted 107. Pertinent information includes, but is not limited to, organization identification, document serial number, public key, secret identification information, document security information, etc., and additional information inserted 109. Additional information includes, but is not limited to, approval, distribution, routing, archival, or embedded document application information, and that the document is made ready for use.

If the system is closed, the application checks whether a central database is accessible 115. If so, the pertinent information is obtained and inserted in the document 117, and the process continues normally at step 105. If the central database is not accessible, the process continues at step 105.

If the VIP does not contain pertinent data, a low-level or uncontrolled document is created, and the process continues at step 109.

Consequently, the present invention, contrary to a closed environment where all of the pertinent information and additional information is self-contained and often centralized, provides a system and method where the document itself includes such information, and thus the relevant and additional information is decentralized. The advantage is that documents can be approved, exchanged, printed, distributed, etc., more freely, while at the same time keeping a minimum amount of security.

More specifically, in the present invention, the document contains information about the signer, and information about the origin of the document.

The contents of the document can be encrypted, and the access to this document can be controlled.

Alternatively, the document approval can be completed in a closed environment only. The document is a secure document, which means it can only be approved in a controlled environment. However, today many people have mobile computers and they are working when not connected to a network or off site. Since the document is supposed to be approved in a secure environment, this creates a problem. As mentioned previously, the security information can be loaded into the document at creation, then security checks can be conducted with information contained in the document. This is a procedure where the document is created outside the closed environment and then enters the closed environment for approvals to be finalized therein. Here, the users will approve the document outside and then approval will be kept pending until the document enters the closed environment and the appropriate security checks are conducted.

Accordingly, the following steps can be followed:

- The document is created outside closed environment
- Optionally, the document could contain a marker indicating whether the document is a secure document or if document will contain pending approvals
- Document is transmitted outside the closed environment
- Document approval will insert approval token into document with an incomplete indicator
- During approval, if any security breaches occur, for example if the password entry is incorrect, this is recorded into the audit trail in the document
- Once the document is introduced back into the closed environment, the security checks for the approval are conducted; if the security checks for approvals are successful, the approval is completed or else the approval is rejected
- Optionally, this method would work for closed and open environment, when the document enters an open environment: the approval entered

will become pending and only completed when entering the closed system.

In addition, this invention discloses a method for embedding applications in the document, Embedded Document Application (EDA) as shown in Figure 4. The EDA's are able to install and execute the application from inside the document. Consequently, an advantage of the present invention is that a user receiving a document created according to the invention does not require an external application to access all these approval and security functions or any other function a document may contain. The document itself will contain the application, or a link to facilitate obtaining the application that is required to achieve all of the required functions. Additionally, the application can establish control with a central database directly or via email or another method to synchronize activity. If, for example, only a certain number of hardcopies of a document can be printed (see Figure 5), the application contained in the document or the external approval application will access security information within the document 301. A determination will be made as to whether secure printing is enabled 303. If so, a determination is made as to whether a central database (or other central location) is accessible 305. If the database is accessible, the print counter is checked 307. If the counter is less than or equal to a predetermined number (meaning that the document can be printed), the print counter is incremented by one 309, security information verified and inserted 311 and the document printed 313.

If secure printing is not enabled, the document can be freely printed. Consequently, security information is verified 319, and the document is printed 321.

If the central database is not accessible, verification cannot be performed and so the print command is aborted 317. Similarly, if the print counter is greater than the predetermined number, the print command is absorbed 317.

In the present invention, a central database is used and the access to this database can be through direct connection, email, internet and/or the web. Similarly, messages to be displayed could be embedded in the document as are the commands on how and where to display them. Optionally, the document could contain an application (another EDA) that could learn information about the use and handling of the document. For example, this other EDA could determine the workflow of the document as it is routed from person to person. This information can then be stored in a central access area. When a new document is created, the EDA in the new document checks this central access area for details pertaining to workflow for this document and then uses this information to route the new document. Modifications and changes can be added to the central data access area. Optionally, the document could have embedded details of how and when it should be routed and distributed. This would enable the EDA to determine if the document cycle has been progressing according to plan i.e. the EDA could determine if the document has been approved by someone at pre-determined time etc. If not, appropriate notification can be sent to a central database and appropriate action could be initiated. Then, the appropriate user can be notified about the document and appropriate action can be taken. It is also possible to update or modify the actions that could be taken by the EDA application via the central database. The document and the EDA could also, depending on the contents of the document, verify the validity of the user's VIP file or could demand a co-signer with appropriate VACs. All this can be done dynamically and is a matter of designing the appropriate structure to meet predetermined objectives.

Referring now to Figure 4, if a document contains an EDA, the system determines if the application is present on the system 201. If not, the application is loaded 203, registered on the system 205 and may be optionally installed on the user system 207. According to the EDA, approval 209, process and behaviour functions 211, security 213, or advertising, branding, corporate logos, etc. 215, actions are performed, and then the EDA is stored 217. The EDA can exhibit different behaviour based on various criteria. For example, a corporation could embed an EDA into their documents that will contain security information, workflow information and also have the corporate logo. The corporation could have another document that could contain the corporate logo and advertising, that it might choose to send out to prospective customers. The EDA can be tailored to have all or some of the functionality described above.

The EDA application contains all the data and executable code. All this information is embedded in the document. When the document is opened the EDA object will load its executable code into memory and execute the code. Optionally, this code could access data from a central database and change, modify and/or update data and functions. Optionally, EDA could load a small application into memory that can execute continuously on the system; this application can monitor all other documents that enter this system and perform the functions of the EDA or activate the document EDA in the document. This will address the issue of a document not being opened by the user. The EDA application can have the capability of self promotion, such as the ability to inform the users where to find the application or to add the application to new documents.

Secure Document Distribution

Once the document has been created and approved, distributing the document can be done using the following methods – electronic distribution or paper distribution or a combination of the two. Ideally, as mentioned earlier, it is best to eliminate paper altogether, however, there are situations where paper will nonetheless be required.

In electronic transmission of the document, if the document contains sensitive materials, then it is highly advisable for the document to be encrypted during distribution. Once again, as mentioned earlier, the encryption can be done using the keys supplied in the VIP file. For example, if the public key of the reader is known, the document can be encrypted with this public key and the recipient can only open it with their private key. Another option is to encrypt with the public key of an organization, then only people who have the private key of the organization can decrypt the document. There are variations on this theme can be used including certificates etc.

When going to paper, the document will be verified by the EDA or the approval application before placing a high quality signature on the document. The approval applications will not place a high quality signature, branded image or seals in the document for printing unless the contents are verified. The approval application will store low quality signature images or no signature images in the document when the document is closed or when the contents have been altered.

BEST MODE IMPLEMENTATION

A user generates VIP files from controlled locations. Appropriate VACs are generated based on the security required by the document. The basic public information such as Name, Address and Telephone numbers are added. Additional private information such as Social Security Number, Driver's license, Passport, Medicare numbers can be added. Additional identification information such as picture, signature, biometric information could also be added to the file. As mentioned above, the more validated data the higher the VAC.

A very minimal VIP file creation would be the following. A user's signature is digitized, a private/public key pair is generated, the application generates a certificate and inserts it into the VIP file (See Figure 1). Additional certificates if available could also be included into the file. The entire file is then encrypted and protected using a user supplied password. The application at a controlled location used to generate the VIP file can be given a certificate, and all subsequent files created at the controlled location will add this certificate to all VIP files or the application can be used with a default certificate. As mentioned earlier additional certificates can be added to this file. If other certificates are used, the public keys of these Certificate Authorities must be accessible to the approval application to verify the certificates; these public keys could be available through a central data base or these keys could be distributed through the embedded data contained in the documents.

A document is created for approval and distribution. If the document is a controlled document, appropriate security information can be embedded into the document, along with an EDA that will have the approval and possibly other functions. Optionally, if this electronic document is an official document, then company letterhead/identification information will be embedded into the document.

Upon initiating an approval, the EDA application will request the person to supply their VIP file or enter an electronic signature. If the document requires biometric verification, this could be requested by the EDA and compared with the stored biometric data in the VIP or a central database or in the document etc. If everything is in order the signature is entered into the document along with other approval information. The information is stored in a secure encrypted fashion.

In a preferred embodiment of the invention, the signature is stored using a special low quality format or a secure reduced noise format. In this last format, the hash of the document is preferably used to create a noise pattern which is filtered to various gradients – depending on the quality required - and then combined with the signature bitmap. This will render the signature on a gray murky background. In order to remove the gray murky background, i.e. noise, the DAC from the document has to be re-calculated and used to clean up the noise. If the DAC has been altered from the time of signing then the noise pattern will not be the same as when it was stored; therefore the background will not be able to be completely removed. This is a secure way to bind the clean signature to the contents of the document. This is only one possible method, other methods could use other forms of encryption to store and secure the contents and signatures together are readily available. It is possible to encrypt the signature and approval information using PKI system or symmetric password based system.

The EDA could display the signature, branded image or could display other information as well, such as advertising, corporate logos, messages etc. Once the EDA has been used to sign the document, the signature will remain in a safe state – in this state the signature will not be displayed in high quality mode unless verified. The signature will only be displayed in a high quality mode if the document contents have not been altered from the time it was signed. Furthermore, if the user tries to print the document, the signature will not print in high quality mode unless the document has been verified to be valid. Once the document has been verified as valid, the EDA will display or print a high quality signature.

The EDA can display other information in the document such as advertising, corporate logos, messages etc. It is possible for this information to be updated periodically via a central database. This will enable the advertising, logos and messages to be updated dynamically, and the updates could be targeted to the actual users. The advertising or messages could be different for each person – if this is desired.

Once the document has been signed it can be emailed to the next user. Again, if the document contains an EDA for signing then the next user can open the document and would be able to work with the signed document. If they have a separate approval application they will also be able to work with the signed document.

If however, the document now needs to go to paper for paper distribution, the user can electronically print the document, the EDA or the approval application will verify the contents of the document and then if the verification is valid, it will print the document with the signatures.

In this implementation the signature is used as the control feature for the document. If the users needs to see or print the document with the signature, the EDA has to verify the document and only then will it display the high quality signature; otherwise the signature is displayed in low quality mode (note: the signature could be alternatively completely removed). It is also possible to use the EDA without any signatures but to use images that are part of a branded identity, such as corporate logos to achieve the same results. For example the EDA could display a watermark indicating the document is invalid - this watermark will only be removed by the EDA if the document contents are verified.

In a preferred embodiment of the invention, the EDA can be used in the following manner. An VIP, which is preferably a representation of a logo, is applied to a document, email message, web page or other electronic media. Certain elements of the VIP are tied to the document, email message, web page or other electronic media. The document, email message, etc., is sent to another user or viewed by another user. If between the time the VIP elements were introduced and tied to the document and the subsequent receipt or viewing of the document, the document was modified, the EDA will not display the logo properly (i.e. with an indication that the document has been modified), or will not display it at all. Consequently, the present invention can enable companies to create secure electronic letterhead with which the company can promote its identity electronically, without fear of somebody simply cutting and pasting the logo from one document to another and therefore passing it off.

Advantageously, unlike paper-based letterhead, the present invention can provide an intelligent letterhead (or logo), which can have multiple views. For example, company A has created dynamic logo A, which includes slogan A1, followed a few seconds later by slogan A2 and then slogan A3, which cycle again. This intelligent logo is then tied to an electronic document according to the method and system of the present invention. A recipient of the document will be able to verify that the document has not been modified since its creation, or has been modified according to established criteria (for example, multiple signings). However, should a person cut and paste the logo from the original document to another document, the logo will invalidate itself and indicate that the logo and the document to which it is attached are not genuine.

It should be understood that the logo is intimately tied to the VIP of the company, and is inserted into a document through an EDA.

Alternatively, the EDA can also be used to function as a security unit. Users do not typically encrypt most email messages. This is mostly due to ignorance of the danger that exists there and the relative difficulty of using encryption software. The EDA application can be used to achieve this in a single step. When creating the document, the users can specify if the document is specific to one person or if access to this document is limited to employees of a certain organization. If the document is meant for one person, the EDA could encrypt the contents using the public key of the intended recipient. Once the intended recipient receives the document the EDA will request that the person supply their VIP file; this will contain the private key required for decrypting the data. Similarly, if the document is meant for employees of a particular organization the contents could be encrypted using the public key of the organization; anyone wishing to access the contents must have the organizations private key. (Note: this private/public key pair could be used just for documents – otherwise there could be a security risk if multiple people have the private key). Key management could also be accomplished by using the EDA; after a certain period of time all users could be forced to a central database for updating their VIP files; during this time appropriate keys could be replaced or updated.

Accordingly, the present invention also provides a system for creating, approving and distributing secure document. The system includes a central location 401 (but could include more than one as mentioned previously). The central location 401 is adapted to store and update a plurality of VIPs which can be created at the central location or other authorized location. Each of the VIPs are linked to a single user (such as a person or corporate organization). The VIP, as mentioned above, includes at least personal information, identity verification data, and a VAC.

The system includes at least one application 403 for creating a document. The application is in communication (which is meant to include intermittent or sporadic communication, such as for a mobile user) with the central location through a network 402. the application is adapted to verify if the VIP of the user creating the document contains pertinent information, and to insert such pertinent information into the document, and to approve the document once created. If the system is closed, it can also include a central database 405 which can also include pertinent information.

If, however, the VIP does not contain pertinent information, then a low-level document is created.

In a preferred embodiment of the invention, the document also includes approval, distribution, routing, archival, or EDA information. Consequently, an advantage of the present invention is that the document itself includes all of the above information. Consequently, the document can travel within closed and open systems, all the while maintaining a minimum level of security.

Consequently, when the document is sent to a recipient application 407, such as another user (through e-mail), a fax machine 409 or a printer 411, the recipient application 407 does not need to recognize what type of document it is and how to handle it. In fact, the document itself contains such information, either through the VIP or through an EDA. When action is to be taken with the document, such as printing, the appropriate verifications are performed based on the information contained in the document.

It should be understood that the recipient application can be just about anything, including an electronic storage media (i.e. CD-ROM, DVD, etc.).

The following definitions are helpful in understanding the present invention.

Definitions:

Approval Data: In general approval data includes information about the person approving, DAC of the document, Audit trail, signatures, biometric information, etc. All or some of the information could be present. This data is usually encrypted for security reasons.

Distribution System: Distribution system implies various methods of distributing data such as email, networks, world wide web, transactions in a transaction processing system, messages or links etc. Distribution system involves using any or all, or combination of systems.

Electronic Document: Electronic Document can represent electronic files composed of text, images, video, graphics, audio, email or any other data or a combination of all of the above. The Electronic document can also contain multiple files containing all or some of the above mentioned items.

Although the present invention has been explained hereinabove by way of a preferred embodiment thereof, is should be pointed out that any modifications to this preferred embodiment within the scope of the appended claims is not deemed to alter of change the nature and scope of the present invention.

CLAIMS

1. A method for creating a virtual identification profile (VIP), comprising the steps of:
(a) obtaining personal information of a user for whom the profile is being created;
(b) obtaining identity verification data;
(c) obtaining relevant data;
(d) updating and editing the information gathered at steps (a) to (c) and calculating a variable authentication code related to this information; and
(e) encrypting the VIP.

2. A method according to claim 1, wherein said method further includes the step of updating a central location with the information contained in the VIP, determining if the update has been successful, and if so marking the central location accordingly, and if not, marking the central location accordingly.

3. A method according to claim 2, wherein said method further includes the steps, prior to step (a), of determining if the VIP is a new VIP, and if so, bypassing steps (a) to (c) and executing directly steps (c) to (f).

4. A method for creating a secure document comprising the steps of:
(a) obtaining a virtual identification profile for the user creating the secure document;
(b) determining if the virtual identification profile includes pertinent information;
(c) if so, inserting pertinent information from the virtual identification profile into the document and making the document ready for use;
(d) if not, creating a low level document and making the document ready for use.

5. A method according to claim 4, wherein said method further includes the step of first determining if the document is being created in a closed environment, and if so determining if the database is available and obtaining from the database pertinent information and inserting the same into the document and then proceeding with step (b); if the document is not being created in a closed environment, proceeding to step (b); and if the database is not available, proceeding to step (b).

6. A method according to claim 5, wherein said method further includes at step (c) inserting additional information into the document.

7. A method according to claim 5, wherein said method further includes at step (d) inserting additional information into the document.

8. A method according to claim 6, wherein said step of adding additional information further includes the step of adding approval, distribution, routing, archival or embedded document application information.

9. A method according to claim 7, wherein said step of adding additional information further includes the step of adding approval, distribution, routing, archival or embedded document application information.

10. A method according to claim 4, wherein said method further includes the step (e) approving the document.

11. A method according to claim 10, wherein said step (e) of approving the document includes the step of inserting into a document an EDA.

12. A method according to claim 11, wherein said VIP includes an electronic signature which can be verified by said EDA.

13. A method according to claim 11, wherein said VIP contains a dynamic logo, and said EDA displays said dynamic logo if the document has not been modified from the time the VIP has been tied to the document and the time the document is viewed.

14. A method for securely printing a secure document including security information, comprising the steps of:

(a) providing the document within an application;

(b) accessing security information present in the document or associated therewith;

(c) determining if secure print is enabled;

(d) if not, verifying and inserting security information and printing the document; or

(i) if so, determining if a central database is available;

(1) if not, aborting the print and informing the user;

(2) if so, verifying if the print counter is less than a predetermined counter;

if not, aborting the print and informing the user; and

if so, incrementing the print counter, verifying and inserting security information and printing the document.

15. A system for creating, approving and distributing secure documents comprising:

a central location for storing and updating a plurality of virtual identification profiles (VIP), each of said virtual identification profiles being linked to a single user, said virtual identification profile including personal information, identity verification data and relevant data, and a variable authentication code associated with a respective VIP; and

at least one application for creating a document, said at least one application being in communication with said central location, said application verifying if said VIP contains pertinent data for the user and for inserting the pertinent data into the document at the time of creation and for approving the document once created.

16. A system according to claim 15, wherein said system is a closed system, and wherein said system further includes a database storing pertinent information; so that said pertinent information is inserted into said document at the time of creation.

17. A system according to claim 15, wherein said system is an open system, and wherein, when it is determined that the VIP does not contain pertinent information, said system creates a low level document.

18. A system according to claim 16, wherein the document includes approval, distribution, routing, archival or embedded document application information.

19. A system according to claim 15, wherein the system further includes at least one printer, and said application further includes a module for determining whether the security information associated with the document permits printing of the document, whether securing printing is enabled, whether a central database is accessible, and whether a print counter is less than a predetermined number, and for incrementing the print counter when the document is printed.

20. A system according to claim 15, wherein the system further includes a recipient application, and wherein said system includes a module for determining if the document can be transmitted to the recipient application.

21. A system according to claim 20, wherein said recipient application is a fax.

22. A system according to claim 20, wherein said recipient application is an email package.

23. A system according to claim 20, wherein said recipient application is a electronic storage media.

24. A system according to claim 15, wherein said system further includes embedding into the document an embedded document application.

25. A system according to claim 24, wherein said VIP includes a dynamic logo, and wherein said EDA displays said dynamic logo if said document has not been changed from the time the VIP is tied to the document to the time the document is viewed.

26. A system according to claim 24, wherein said VIP includes a signature, and wherein said EDA displays said signature in a clear form if said document has not been changed from the time the VIP is tied to the document to the time the document is viewed, or displays said signature in a clear form if said EDA determines that said document has been modified according to predetermined criteria.

Current Hybrid Document Environment

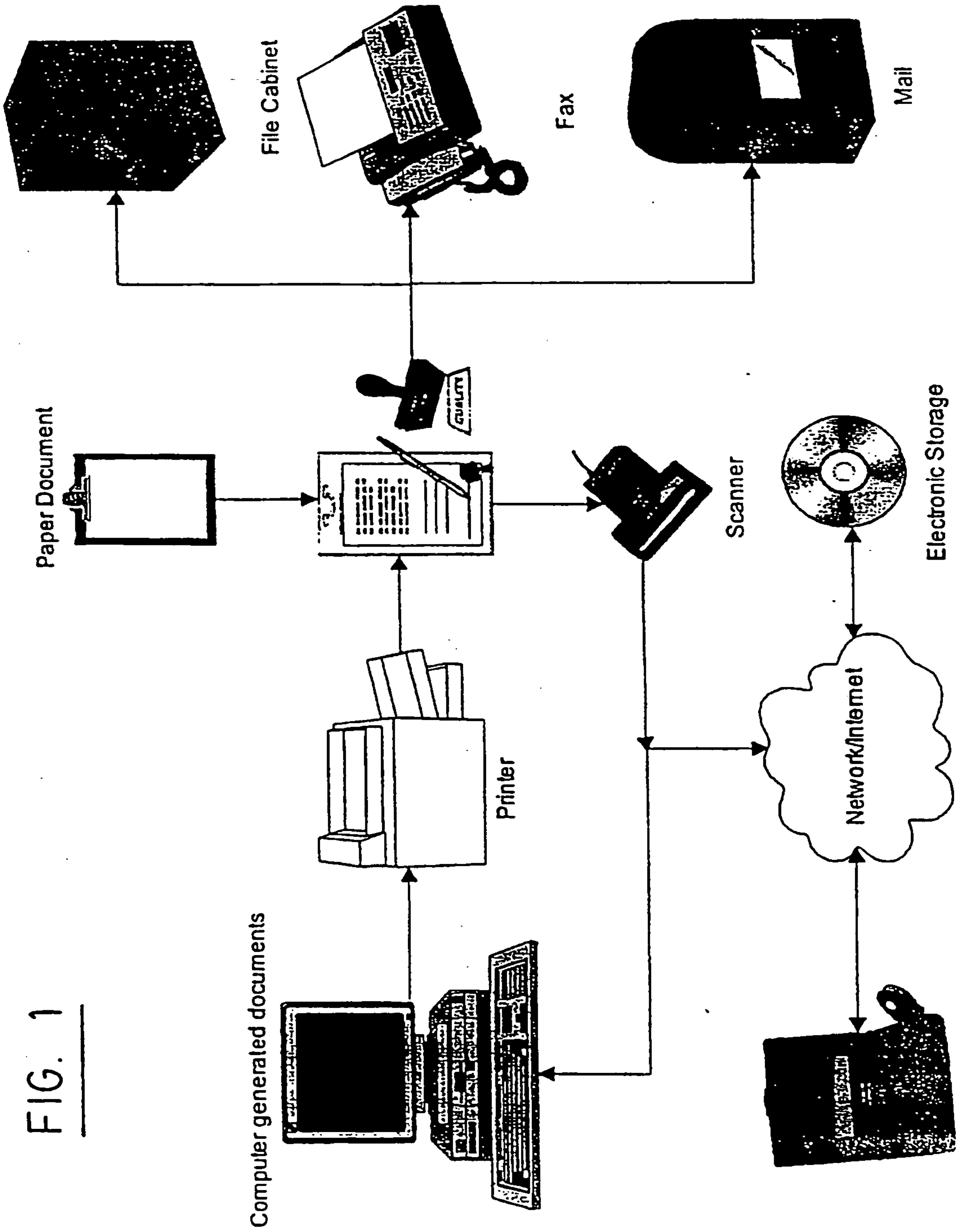


FIG. 1

CREATING THE VIRT. .L IDENTIFICATION PROFILE (VIP)

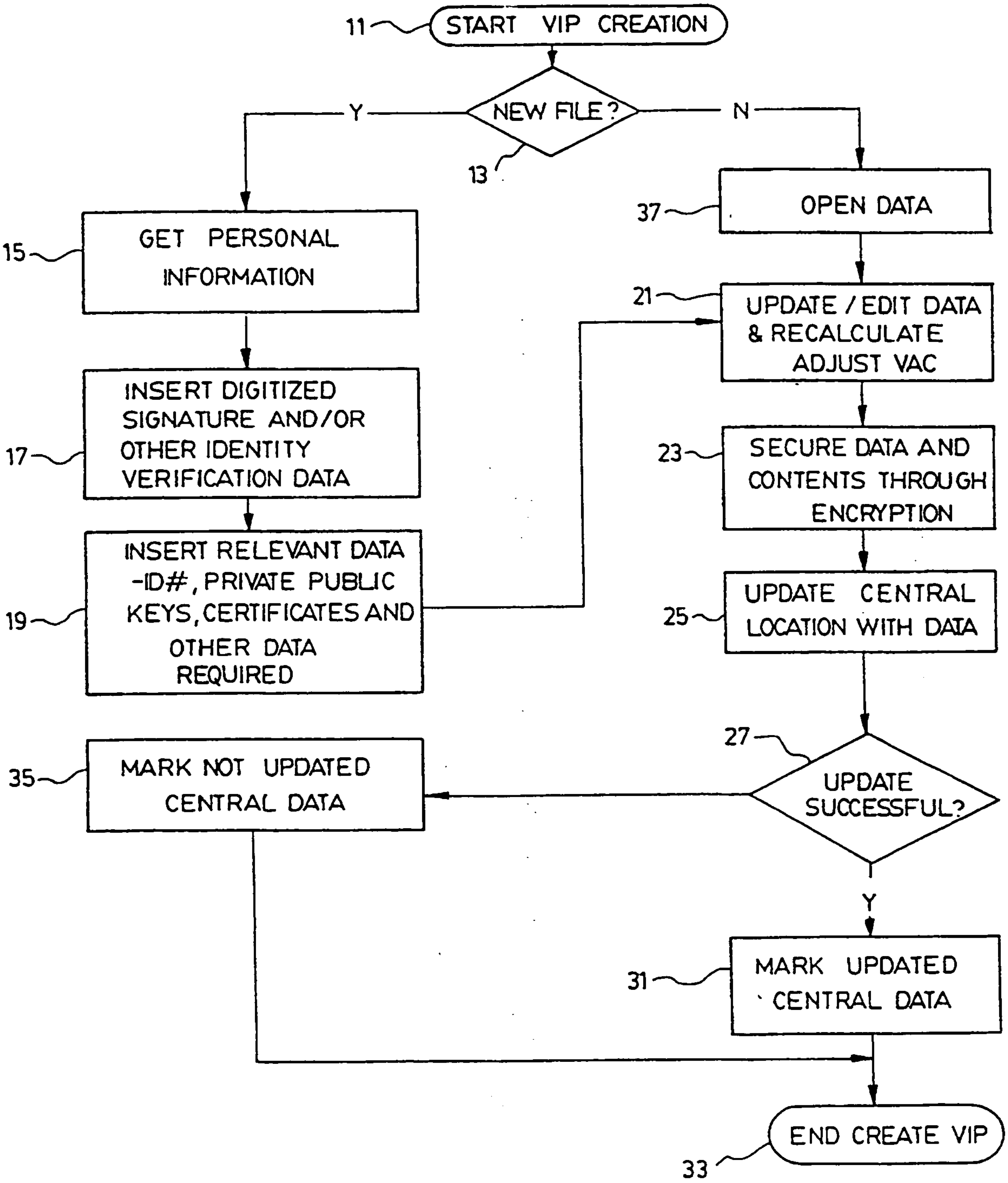

11
START VIP CREATION
NEW FILE?
13
Y
N
15
GET PERSONAL INFORMATION
17
INSERT DIGITIZED SIGNATURE AND/OR OTHER IDENTITY VERIFICATION DATA
19
INSERT RELEVANT DATA -ID#, PRIVATE PUBLIC KEYS, CERTIFICATES AND OTHER DATA REQUIRED
37
OPEN DATA
21
UPDATE / EDIT DATA & RECALCULATE ADJUST VAC
23
SECURE DATA AND CONTENTS THROUGH ENCRYPTION
25
UPDATE CENTRAL LOCATION WITH DATA
27
UPDATE SUCCESSFUL?
35
MARK NOT UPDATED CENTRAL DATA
Y
31
MARK UPDATED CENTRAL DATA
END CREATE VIP
33

FIG. 2

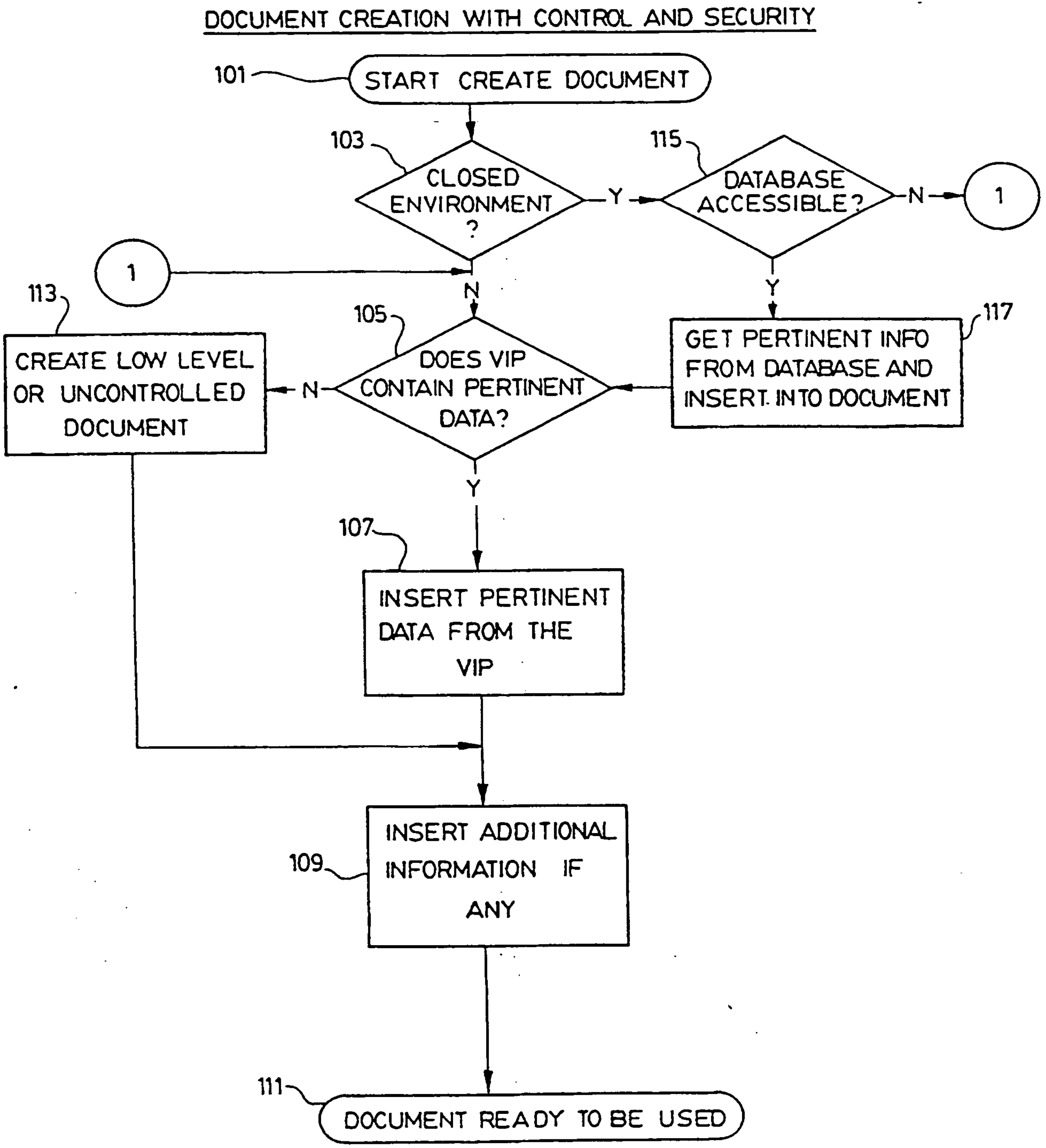

DOCUMENT CREATION WITH CONTROL AND SECURITY
101
START CREATE DOCUMENT
103
CLOSED ENVIRONMENT ?
Y
115
DATABASE ACCESSIBLE ?
N
1
1
N
Y
113
105
117
CREATE LOW LEVEL OR UNCONTROLLED DOCUMENT
N
DOES VIP CONTAIN PERTINENT DATA?
GET PERTINENT INFO FROM DATABASE AND INSERT INTO DOCUMENT
Y
107
INSERT PERTINENT DATA FROM THE VIP
109
INSERT ADDITIONAL INFORMATION IF ANY
111
DOCUMENT READY TO BE USED

FIG. 3

EMBEDDED DOCUMENT APPLICATION (EDA)

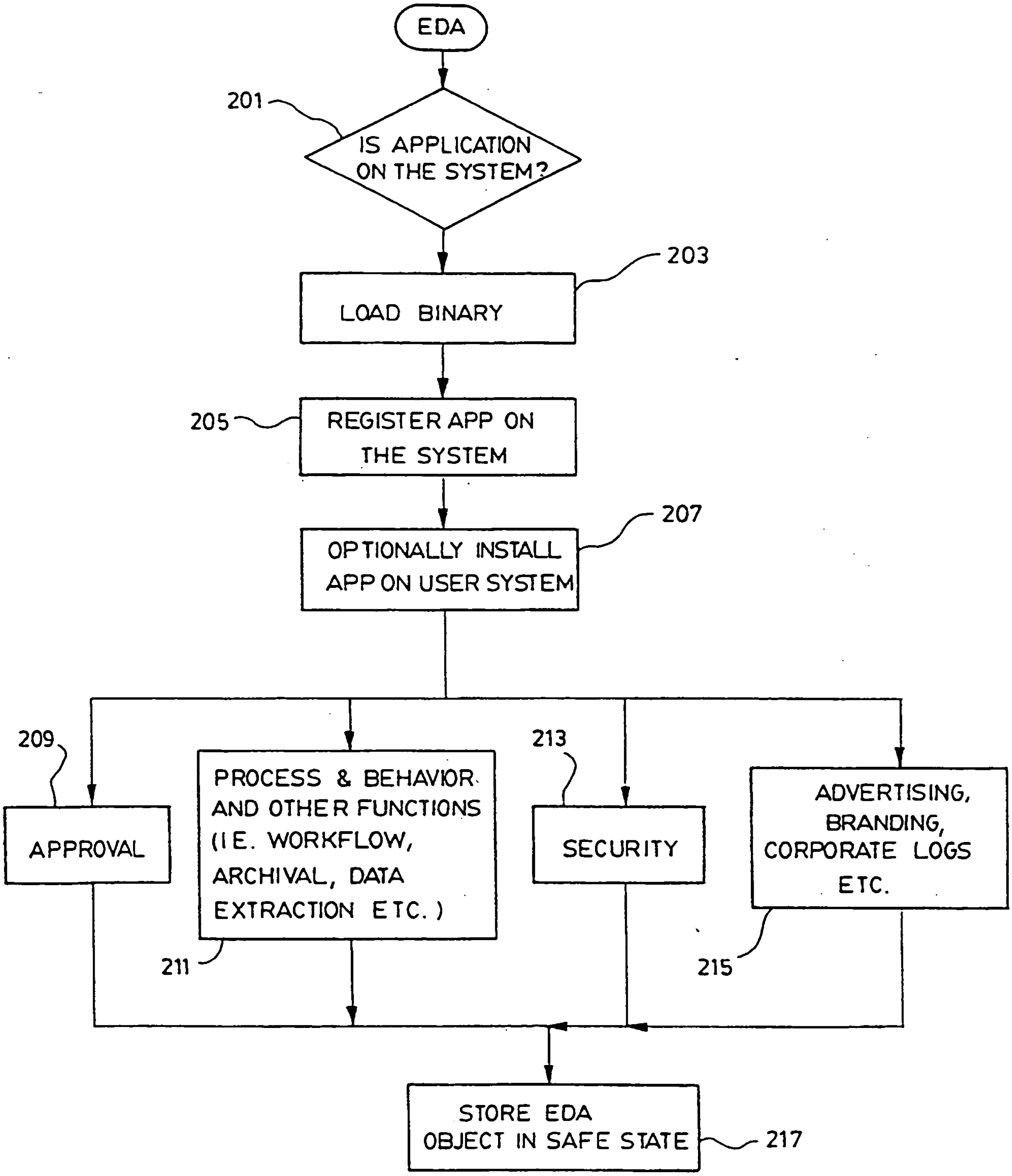

EDA
201
IS APPLICATION ON THE SYSTEM?
203
LOAD BINARY
205
REGISTER APP ON THE SYSTEM
207
OPTIONALLY INSTALL APP ON USER SYSTEM
209
APPROVAL
PROCESS & BEHAVIOR AND OTHER FUNCTIONS (I E. WORKFLOW, ARCHIVAL, DATA EXTRACTION ETC.)
211
213
SECURITY
ADVERTISING, BRANDING, CORPORATE LOGS ETC.
215
STORE EDA OBJECT IN SAFE STATE
217

FIG. 4

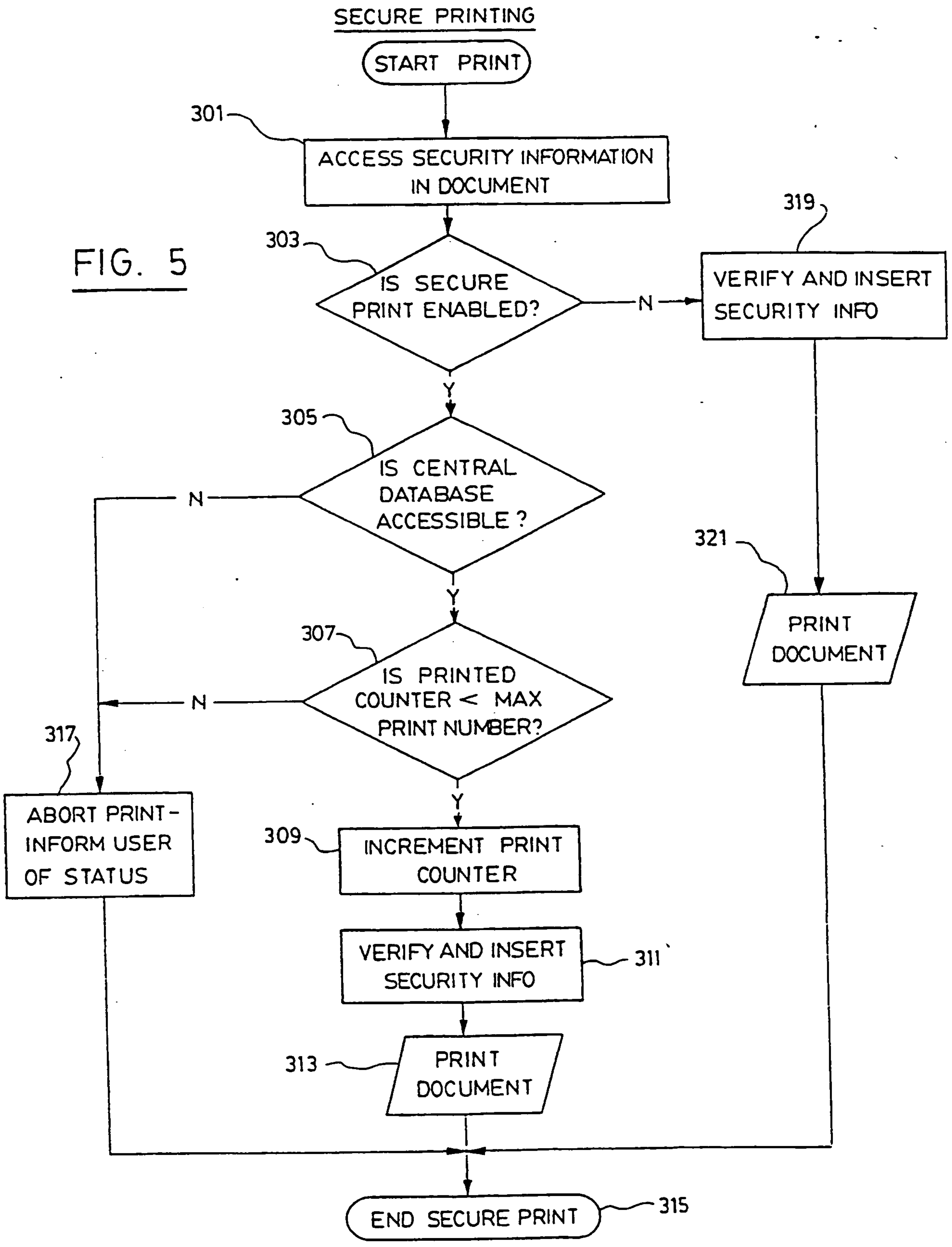

SECURE PRINTING
START PRINT
301
ACCESS SECURITY INFORMATION IN DOCUMENT
303
IS SECURE PRINT ENABLED?
N
Y
319
VERIFY AND INSERT SECURITY INFO
305
IS CENTRAL DATABASE ACCESSIBLE ?
N
Y
321
PRINT DOCUMENT
307
IS PRINTED COUNTER < MAX PRINT NUMBER?
N
Y
317
ABORT PRINT - INFORM USER OF STATUS
309
INCREMENT PRINT COUNTER
VERIFY AND INSERT SECURITY INFO
311
313
PRINT DOCUMENT
END SECURE PRINT
315

FIG. 5

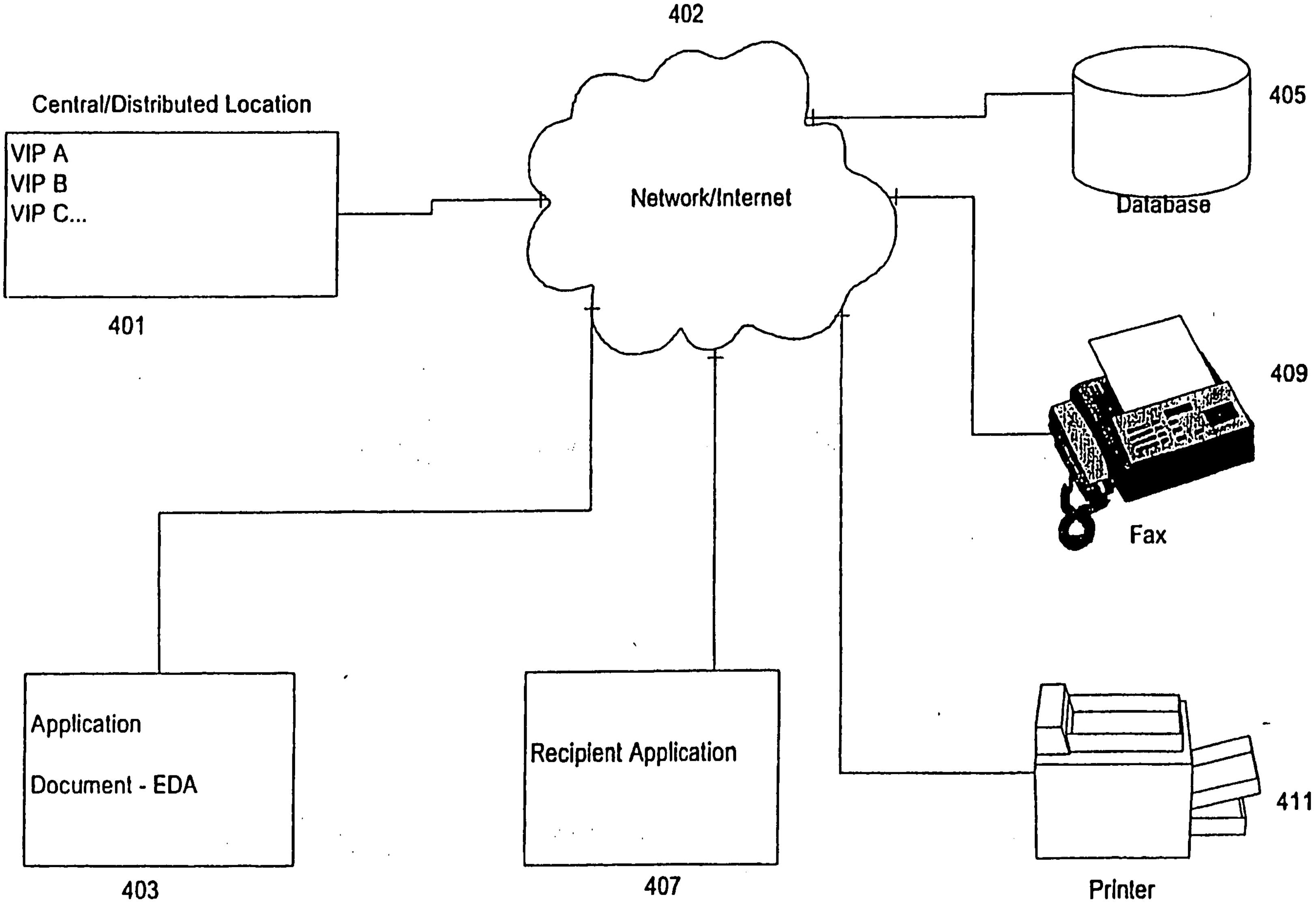

Central/Distributed Location
VIP A
VIP B
VIP C...
401
402
Network/Internet
405
Database
409
Fax
Application
Document - EDA
403
Recipient Application
407
411
Printer

FIG. 6

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 October 2000 (19.10.2000)

PCT

(10) International Publication Number
WO 00/62140 A3

(51) International Patent Classification⁷: G06F 17/60, 17/24

(21) International Application Number: PCT/CA00/00406

(22) International Filing Date: 12 April 2000 (12.04.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/128,871 12 April 1999 (12.04.1999) US

(71) Applicant: **SILANIS TECHNOLOGY INC.** [CA/CA]: 3333 Côte Vertu, Suite 450, St-Laurent, Quebec H4R 2N1 (CA).

(72) Inventors: **SILVESTER, Joseph**; 282 Place des Cèdres, Dollard des Ormeaux, Quebec H9G 1W1 (CA). **PETROGIANNIS, Tommy**; 4560 Cumberland Avenue, Montreal, Quebec H4B 2L4 (CA). **LEBLANC, François**; 3770 Ave. Laval, Montreal, Quebec H2W 2H7 (CA). **DUMAIS, Guy**; 9181 Millen, Montreal, Quebec H2M 1W8 (CA). **GOUDREAULT-EDMOND, Benoit**; 7349 Ave. Azilda, Anjou, Quebec H1K 3A4 (CA). **LAURIE, Michael**; 4827 Meloche, Pierrefonds, Quebec H9J 1Y9 (CA). **MILCZAREK, Ed**; 5135 des Cageux, Pierrefonds, Quebec H9J 3C4 (CA).

(74) Agent: **ROBIC**; 55 Saint-Jacques, Montreal, Quebec H2Y 3X2 (CA).

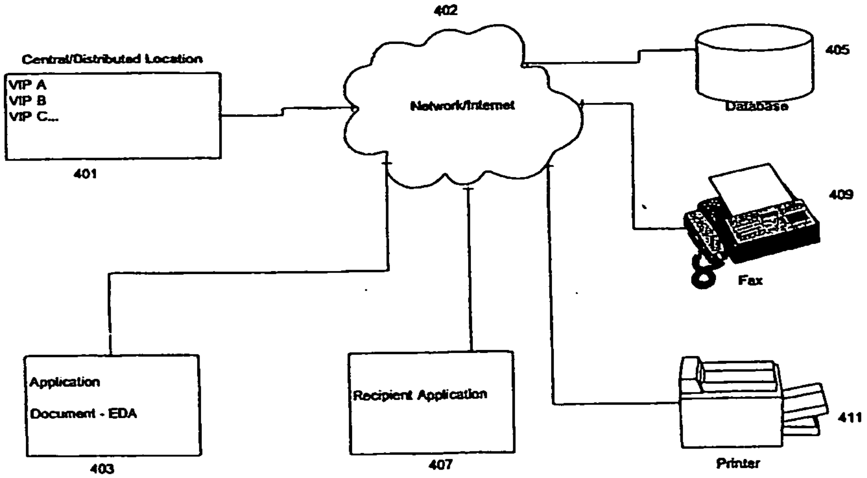
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SECURE ELECTRONIC DOCUMENT CREATION, APPROVAL AND DISTRIBUTION METHOD IN AN OPEN AND DISTRIBUTED NETWORK ENVIRONMENT



(57) Abstract: The invention concerns a system and method for the secure creation, approval and distribution of electronic documents in an open and distributed network environment. Personal information of a user for whom a profile is being created; identity verification data; and relevant data regarding the user are obtained in order to create a virtual identification profile (VIP). The information is updated and edited and a variable authentication code (VAC) related to this information is calculated. The VIP is then encrypted, and a central location is updated with the information. The VIP can be used in a system which includes a central location for storing and updating a plurality of VIPs, and at least one application for creating a document, the application being in communication with the central location. The application verifies if the VIP contains pertinent data for the user and for inserting the pertinent data into the document at the time of creation and for approving the document once created.

(88) **Date of publication of the international search report:** 30 August 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/CA 00/00406

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/60 G06F17/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

WPI Data, EPO-Internal, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 565 314 A (FISCHER) 13 October 1993 (1993-10-13) the whole document ---	1
A,P	WO 00 19296 A (SILANIS TECHNOLOGY INC.) 6 April 2000 (2000-04-06) the whole document ---	1
A,P	WO 00 19315 A (SILANIS TECHNOLOGY INC.) 6 April 2000 (2000-04-06) the whole document ---	1
A,P	WO 00 19295 A (SILANIS TECHNOLOGY INC.) 6 April 2000 (2000-04-06) the whole document --- -/--	1

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 27 March 2001	Date of mailing of the international search report 04/04/2001
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Abram, R

1

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/CA 00/00406

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A,P	WO 00 08541 A (SILANIS TECHNOLOGY INC.) 17 February 2000 (2000-02-17) the whole document -----	1

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int· tional Application No
PCT/CA 00/00406

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 565314 A	13-10-1993	AT 198800 T	15-02-2001
		AU 3560793 A	07-10-1993
		CA 2093094 A	07-10-1993
		DE 69329869 D	22-02-2001
		EP 1031908 A	30-08-2000
		JP 6295286 A	21-10-1994
		US 5390247 A	14-02-1995
		US 5337360 A	09-08-1994
WO 0019296 A	06-04-2000	AU 5844699 A	17-04-2000
WO 0019315 A	06-04-2000	AU 5844499 A	17-04-2000
WO 0019295 A	06-04-2000	AU 5844599 A	17-04-2000
WO 0008541 A	17-02-2000	AU 5144499 A	28-02-2000